Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Communications Acquisitions Corporation d/b/a Whaleback Managed Services ("Whaleback") began providing service in December 2011. Accordingly, this Annual 64.2009(e) CPNI Certification for 2011 applies only to the company's operations during December 2011.

1. Date filed: April 4, 2012

2. Name of company(s) covered by this certification: Communications Acquisitions Corporation d/b/a Whaleback Managed Services

3. Form 499 Filer ID: Whaleback recently began providing service, and has not yet been issued a Form 499 Filer ID. Whaleback's FCC Registration Number is 0021623681.

4. Name of signatory: Karil Reibold

5. Title of signatory: CEO

6. Certification:

I, Karil Reibold, certify that I am an officer of the company named above, that I am acting as an agent of the company, and that, to the best of my personal knowledge, the company has established operating procedures designed to ensure compliance with the Commission's CPNI rules contained in 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures during the certification period were designed to ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

Signed Karil Reibold

Attachments: Accompanying Statement explaining CPNI procedures

Statement Regarding the Customer Proprietary Network Information (CPNI) Procedures of Communications Acquisitions Corporation d/b/a Whaleback Managed Services

This statement summarizes the internal policies and procedures of Communications Acquisitions Corporation d/b/a Whaleback Managed Services ("Whaleback") concerning its compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules, 47 C.F.R. § 64.2001 *et seq.* (the "CPNI Rules").

USE OF CPNI – SECTION 64.2005

Whaleback may from time to time use, disclose, or permit access to CPNI for the purpose of providing or marketing services among the same categories of service to which the customer already subscribes from Whaleback or as otherwise permitted under sections 64.2005(c) or (d) of the Commission's rules, 47 C.F.R. §§ 64.2005(c), (d), or section 222 of the Communications Act of 1934, as amended, 47 U.S.C. § 222 (the "Act"). Whaleback does not otherwise use, disclose or permit access to CPNI for any other purposes, including marketing the products or services of itself, its affiliates or any third parties. As such, Whaleback does not solicit the approval of customers to use CPNI.

Whaleback does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

APPROVAL OR NOTICE REQUIRED FOR USE OF CPNI – SECTIONS 64.2007 AND 64.2008

Whaleback does not use, disclose or permit access to CPNI for the purpose of marketing the products or services of itself, its affiliates or any third parties, or for any other purpose that would require Whaleback to solicit customer approval or provide notice to customers before doing so. As such, Whaleback does not solicit the approval of, or provide notice to, customers for use of CPNI.

If Whaleback subsequently chooses to take any action for which customer approval or notice is required, the company will implement policies and practices for seeking opt-out or opt-in approval from its customers in accordance with the CPNI Rules obtain approval from its customers pursuant to these policies and practices before taking such action.

SAFEGUARDS REQUIRED FOR USE OF CPNI – SECTION 64.2009

Because the company does not use, disclose or permit access to CPNI for any purpose that would require the company to solicit the approval of customers for use of CPNI, Whaleback does not solicit the approval of such customers. If Whaleback subsequently chooses to take any action for which the company must solicit the approval of its customers for the use of CPNI, the company will implement a system by which the status of the customer's CPNI approval can be clearly established prior to the use of CPNI.

Whaleback has trained its personnel as to when they are and are not authorized to use CPNI, and the company has an established, express disciplinary process that can result in disciplinary actions up to, and including, termination of employment, for failure to comply with the company's CPNI policies.

Whaleback may from time to time use, disclose, or permit access to CPNI for the purpose of providing or marketing services among the same categories of service to which the customer already subscribes from Whaleback or is otherwise permitted under the CPNI Rules or the Act. Whaleback does not use, disclose or permit access to CPNI for any other purpose of marketing the products or services of itself, its affiliates or any third parties, or for any purpose that would require Whaleback to solicit customer approval before doing so. In the cases Whaleback chooses to use, disclose or permit access to CPNI, the company maintains a record of (1) its own and its affiliates' sales and marketing campaigns that use its customers' CPNI, and (2) all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign. Whaleback retains the record for a minimum of one year.

Whaleback has established a supervisory review process regarding its compliance with the CPNI Rules for outbound marketing situations. Whaleback also maintains records of its compliance for a minimum period of one year. Whaleback sales and marketing personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

An officer of Whaleback signs and files with the Commission a compliance certificate on an annual basis. The officer states in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the CPNI Rules. Whaleback also provides a statement accompanying the certificate explaining how its operating procedures ensure that it is in compliance with the CPNI Rules. In addition, Whaleback includes an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. The company makes this filing annually with the Enforcement Bureau for data pertaining to the previous calendar year.

Whaleback does not solicit opt-out approval from its customers for use of CPNI. If Whaleback subsequently chooses to take any action for which the company must solicit the opt-out approval of its customers for the use CPNI, the company will provide written notice within five business days to the Commission of any instance where the opt-out mechanisms do not work properly to such a degree that customers' inability to opt-out is more than an anomaly. The notice will be made pursuant to, and in accordance with, section 64.2009(f) of the Commission's rules, 47 C.F.R. § 64.2009(f).

SAFEGUARDS ON THE DISCLOSURE OF CPNI – SECTION 64.2010

Whaleback has implemented reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.

Whaleback properly authenticates a customer prior to disclosing CPNI based on customer-initiated telephone contact or online account access. (Whaleback has no retail locations and does not disclose CPNI at its office locations.) Specifically, Whaleback requires a customer to provide a predefined

password, if it has been registered, prior to disclosing call detail information over the telephone during customer-initiated telephone contact. Customers that have not defined a password are being contacted to register a password for future calls. Whaleback also requires a customer defined password prior to providing online access to CPNI.

Pursuant to the CPNI Rules, Whaleback authenticates a customer without the use of readily available biographical information, or account information; permits customers to define their own passwords; and notifies customers of account changes to the customer's address on record (which does not reveal the changed information, and it is not sent to the new account information).

Whaleback does not bind itself contractually to authentication regimes other than those described in section 64.2010 of the Commission's rules, 47 C.F.R. § 64.2010, for services the company provides to business customers.

NOTIFICATION OF CPNI SECURITY BREACHES – SECTION 64.2011

Whaleback will notify law enforcement of a breach of its customers' CPNI as provided in section 64.2011 of the Commission's rules, 47 C.F.R. § 64.2011.

Whaleback will not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until the company has completed the process of notifying law enforcement pursuant to paragraph (b) of section 64.2011 of the Commission's rules, 47 C.F.R. § 64.2011(b).

After Whaleback has completed the process of notifying law enforcement pursuant to paragraph (b) of section 64.2011 of the Commission's rules, 47 C.F.R. § 64.2011(b), it will notify its customers of a breach of those customers' CPNI.

Whaleback will maintain a record of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b) of section 64.2011 of the Commission's rules, 47 C.F.R. § 64.2011(b), and notifications made to customers. The record will include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Whaleback will retain the record for a minimum of two years.